THE AMERICAN MATHEMATICAL MONTHLY.

Entered at the Post-office at Springfield, Missouri, as second-class matter.

VOL. X. FEBRUARY, 1903. No. 2.

AN ELEMENTARY EXAMPLE OF MODULAR SYSTEMS.

By PROF. G. A. MILLER.

The following exposition is based upon Kronecker's *Lectures on Number Theory*, pp. 144-150.* While the example is very elementary and does not lead to any new results, yet it may serve to give some idea of the general modular systems, and also to exhibit a fundamental theorem of arithmetic in an attractive manner.

The number† a is said to be divisible by m whenever it is possible to find a number c such that $a=cm$. Similarly we may say that a is divisible by the system of numbers $m_1, m_2, \ldots, m_\alpha$ provided it is possible to find α numbers c_1, $c_2, \ldots, c_\alpha$ such that

$$a=c_1m_1+c_2m_2+\ldots+c_\alpha m_\alpha .$$

From this standpoint the system of numbers $m_1, m_2, \ldots, m_\alpha$ is called a *modular system* and it is denoted by $(m_1, m_2, \ldots, m_\alpha)$. The numbers $m_1, m_2, \ldots, m_\alpha$ are called the *elements* of the system. For instance, 3 is divisible by the modular system (7, 16, 25) because $3=3.7+2.16-2.25$. In particular, zero is divisible by every modular system since

$$0=0.m_1+0.m_2+\ldots+0.m_\alpha .$$

Vorlesungen ueber Zahlentheorie von Leopold Kronecker, Erster Band, Leipzig, 1901, B. G. Teubner.

†Only integers, including 0, are meant by the term *number* as used in this note.

One modular system $(m_1, m_2, \ldots, m_\alpha)$ is said to be divisible by another $(d_1, d_2, \ldots, d_\beta)$ whenever each element of the first system is divisible by the second system; *i. e.*, when the following α equations are satisfied:

$$
\begin{aligned}
m_1 &= c_{11}d_1 + c_{12}d_2 + \ldots + c_{1\beta}d_\beta\,, \\
m_2 &= c_{21}d_1 + c_{22}d_2 + \ldots + c_{2\beta}d_\beta\,, \\
&\cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\
m_\alpha &= c_{\alpha 1}d_1 + c_{\alpha 2}d_2 + \ldots + c_{\alpha\beta}d_\beta\,.
\end{aligned}
$$

For instance, the system (20, 35) is divisible by the system (15, 25, 10) since

$$
\begin{aligned}
20 &= 0.15 + 0.25 + 2.10, \\
35 &= 1.15 + 0.25 + 2.10.
\end{aligned}
$$

From the following equations it follows that the system (15, 25, 10) is also divisible by the system (20, 35):

$$
\begin{aligned}
15 &= 1.35 - 1.20, \\
25 &= 3.35 - 4.20, \\
10 &= 2.35 - 3.20.
\end{aligned}
$$

Two modular systems which have the property that each of them is divisible by the other are called *equivalent*. The above examples prove that the two systems (20, 35) and (15, 25, 10) are equivalent. This relation may be indicated by the symbol $(20, 35) \backsim (15, 25, 10)$. It may be observed that we are here dealing with an interesting *extension of ordinary division*. If each of two equivalent modular systems is composed of only one element these two elements must be equal as in ordinary division.

If a number is divisible by $(m_1, m_2, \ldots, m_\alpha)$ it is evidently also divisible by $(d_1, d_2, \ldots, d_\beta)$, since the latter is a divisor of the former. In particular, if a number is divisible by a given modular system it is also divisible by every equivalent system. If each one of two numbers is divisible by $(m_1, m_2, \ldots, m_\alpha)$ it is evident that their sum and their difference are divisible by the same system; *i. e.*, the multiples of a given modular system reproduce themselves when they are combined with respect to the two operations, addition and subtraction. Hence they must also reproduce themselves with respect to multiplication.

Since the multiples of two equivalent systems are identical, it is of interest to determine the simplest system which is equivalent to a given system $(m_1, m_2, \ldots, m_\alpha)$. It is not difficult to see directly that this consists of a single element, viz. the greatest common divisor of the elements $m_1, m_2, \ldots, m_\alpha$. That is, *each modular system of numbers is equivalent to some modular system composed of one element.* If the elements of the modular system are functions of one or more

variables this result is not generally true.* The following considerations furnish a simple proof of the theorem stated above when $m_1, m_2, \ldots, m_\alpha$ are numbers.

Let m be any number which is divisible by $(m_1, m_2, \ldots, m_\alpha)$ and consider the two systems

$$(m, m_1, m_2, \ldots, m_\alpha) \text{ and } (m_1, m_2, \ldots, m_\alpha).$$

Since every element of each of these systems is divisible by the other system we have $(m, m_1, m_2, \ldots, m_\alpha) \sim (m_1, m_2, \ldots, m_\alpha)$.

That is, *if any multiple of the elements of a modular system be added to its elements the resulting system is equivalent to the original system.*

In particular, the two systems $(m_1+tm_2, m_1, m_2, \ldots, m_\alpha)$ and $(m_1, m_2, \ldots, m_\alpha)$ are equivalent for all values of t. The former of these is clearly equivalent to $(m_1+tm_2, m_2, \ldots, m_\alpha)$ since

$$m_1=(m_1+tm_2)-tm_2.$$

Hence it follows that $(m_1, m_2, \ldots, m_\alpha) \sim (m_1+tm_2, m_2, \ldots, m_\alpha)$.

That is, *any modular system is equivalent to the one obtained by increasing or decreasing one of its elements by any multiple of any other element of the system.*

Suppose that a given modular system involves at least two elements which differ from 0. The preceding theorem enables us to find an equivalent system in which one of the elements is reduced by an integer. Hence every modular system is equivalent to a system in which all the elements except one are zeros. Since two systems which differ only with respect to 0 elements are equivalent, it follows that every modular system is equivalent to a system containing only one element, as was stated above. That is, it is always possible to find a number d such that

$$(m_1, m_2, \ldots, m_\alpha) \sim (d).$$

It remains only to find d. Since each of the elements $m_1, m_2, \ldots, m_\alpha$ is divisible by d it follows that d is a common divisor of the elements of $(m_1, m_2, \ldots, m_\alpha)$. The other condition imposed by this equivalence, viz.,

$$d=c_1 m_1+c_2 m_2+\ldots+c_\alpha m_\alpha,$$

requires that d be divisible by the greatest common divisor of $m_1, m_2, \ldots, m_\alpha$. Hence d must be the greatest common divisor of the elements of

$$(m_1, m_2, \ldots, m_\alpha).$$

We are now in position to see more clearly why the two systems

$$(20, 35) \quad (15, 25, 10)$$

---

*All the modular systems considered in this note are supposed to have numbers for their elements.

are equivalent, as each of them is equivalent to (5).

Suppose that the greatest common divisor of the elements of the system $(m_1, m_2, \ldots, m_a)$ is unity. From

$$(m_1, m_2, \ldots, m_a) \backsim (1)$$

it follows that it is possible to find a numbers $c_1, c_2, \ldots, c_a$ such that

$$c_1 m_1 + c_2 m_2 + \ldots + c_a m_a = 1.$$

In particular, we have the fundamental theorem that it is possible to find two numbers x, y such that

$$m_1 x + m_2 y = 1,$$

whenever m_1 and m_2 are prime to each other.

GENERALIZATION OF A FUNDAMERTAL THEOREM IN THE GEOMETRY OF THE TRIANGLE.

By PROF. M. W. HASKELL.

The theorem in question is of fundamental importance in the geometry of the triangle,* and may be stated as follows:

If A', B', C' be points chosen at will on the sides BC, CA, AB of any triangle ABC, the circles $AB'C'$, $BC'A'$, $CA'B'$ pass through one and the same point O.

In a communication presented to the Chicago Section of the American Mathematical Society January 2, 1902, I extended this theorem to the tetrahedron in the following form:

Let F, G, H, P, Q, R be any points on the edges AD, BD, CD, BC, CA, AB, respectively, of any tetrahedron; the four spheres $AFQR$, $BGRP$, $CHPQ$, $DFGH$ pass through one and the same point O.

The theorem is, however, capable of generalization to space of any number of dimensions without any difficulty. I will therefore state and prove it at once for space of n dimensions,—understanding by a spherical space of three dimensions, S_3, a space every section of which by a flat space of three dimensions, R_3, is an ordinary sphere, and in general by a spherical S_{n-1} a space every section of which by a flat R_{n-1} is a spherical S_{n-2}. A spherical S_{n-1} will evidently be determined by $n+1$ points of which never more than two lie on the same line nor more than three in the same plane, etc. The general theorem may then be stated in the following words:

---

*McClelland, *Geometry of the Circle*, page 40; see also Rouche et de Comberousse, *Traite de Geometrie*, 7th edition, Vol. I, page 486.